REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are unpatentable under the provisions of non-statutory obviousness type double patenting and 35 U.S.C. §§ 101 and 103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. CLAIM OBJECTIONS

The Examiner objected to claims 1-14 due to informalities. Specifically, the Examiner suggested that the term "adapted to" should be amended. Responsive to the Examiner, the Applicants amended claims 1, 6-8 and 13 to amend the term "adapted to." As such, the Applicants request the objection be withdrawn.

II. REJECTION OF CLAIMS 1, 8 AND 15 UNDER 35 U.S.C. § 101

The Examiner rejected claims 1, 8 and 15 under 35 U.S.C. § 101 as being the same as claim 1 of U.S. Patent No. 7,444,417 (hereinafter the '417 patent). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that claim 1 of the '417 patent and the claims 1, 8 and 15 of the present application are not the same. For example, claim 1 of the '417 patent does not refer to any VPNs nor does it recite the limitation of "a VPN application in communication with a first one of said plurality of edge routers, said VPN application having a first IP address" or any limitation about injecting BGP routing instructions. In fact, none of the limitations of claim 1 of the '417 patent and claims 1, 8 and 15 of the present application are the same. Therefore, the Applicants submit that claims 1, 8 and 15 fully satisfy the requirements for double patenting under 35 U.S.C. § 101 and request the rejection be withdrawn.

III. REJECTION OF CLAIMS 1-3, 8 AND 15 UNDER NON-STATUTORY OBVIOUSNESS-TYPE DOUBLE PATENTING

The Examiner provisionally rejected claims 1-3, 8 and 15 as being unpatentable over claims 1, 3, 12 and 14 of co-pending application no. 12/284,254. Responsive to the Examiner, the Applicants herein file a terminal disclaimer to overcome the rejection. As such, the Applicants request the rejection be withdrawn.

IV. REJECTION OF CLAIMS 1-8 AND 10-19 UNDER 35 U.S.C. § 103

The Examiner rejected claims 1-8, and 10-19 as being unpatentable over Talpade, et al. (U.S. Patent Publication No. 2004/0148520, published on July 29, 2004, hereinafter referred to as "Talpade") in view of Munger, et al. (U.S. Patent No. 6,618,761, issued on September 9, 2003, hereinafter referred to as "Munger") and Official Notice. The Applicants respectfully traverse the rejection.

Talpade teaches mitigating denial of service attacks. Talpade teaches rerouting all traffic from all routers to a filter router when a denial of service attack is detected. (See Talpade, Abstract).

Munger teaches an agile network protocol for secure communications with assured system availability. Methods and systems for allowing a plurality of computer nodes to communicate using weighted transmission paths are provided. (See Munger, Abstract).

The Examiner's attention is directed to the fact that Talpade, Munger, and Official Notice, either alone or in any permissible combination, fail to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router, as

positively claimed by the Applicants. Specifically, Applicants' independent claims 1, 8 and 15 positively recite:

1. An internet service provider (ISP) Virtual Private Network (VPN) network comprising:

a plurality of edge routers;

a plurality of core routers for allowing communication between said plurality of edge routers;

a VPN application in communication with a first one of said plurality of edge routers, said VPN application having a first IP address; and

a black-hole router in communication with said plurality of core routers, said black-hole router for injecting a second IP address into said ISP VPN network, said second IP address comprising:

a same IP address as the first IP address;

a higher preference value than said first IP address; and

a community value such that when said second IP address is injected, a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. (Emphasis added).

8. An internet service provider (ISP) network comprising:

a plurality of edge routers;

an application in direct or indirect electrical communication with a first one of said plurality of edge routers;

said application having a first IP address such that Virtual Private Network (VPN) traffic addressed for said first IP address and entering said ISP network at anyone of said plurality of edge routers, is routed to said application;

a black-hole router; and

a router for injecting an instruction into said ISP network, such that one or more select edge routers redirect VPN traffic, which is addressed to said first IP address, to said black-hole router, wherein said injected instruction comprises a routing instruction having a same IP address as said first IP address, but with a higher preference value than said first IP address and having a community value. (Emphasis added).

15. A method of managing a Distributed Denial of Service (DDoS) attack on an application within an internet service provider (ISP) network, said application having a first IP address, said method comprising:

injecting a Border Gateway Protocol (BGP) routing instruction into said ISP network when said DDoS attack is occurring, said BGP routing instruction comprising a second IP address having a same IP address as said first IP address, but with a higher preference value than said first IP

address and having a community value;

redirecting, at one or more selected edge routers, VPN traffic addressed for said second IP address to a black-hole router; and

directing, at one or more other edge routers, VPN traffic addressed for said first IP address to said application that is experiencing said DDoS attack. (Emphasis added).

In one embodiment, the Applicants teach a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. For example, the Applicants teach selectively re-routing traffic of one or more edge routers by using preference and community values of an injected instruction or second IP address that is identical to a first address. (See e.g., Applicants' specification, page 11, line 16 – page 12, line 5).

The alleged combination (as taught by Talpade) fails to render obvious the Applicants' claims because the alleged combination fail to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. First, the Applicants note that Talpade teaches away from the Applicants' claims. The Applicants' disclosure teaches that only a select number of edge routers (i.e., less than all or a subset of all the routers) are instructed to re-direct traffic to the black hole router, while the remaining routers continue to forward traffic to the VPN application. Thus, only some of the VPN traffic is diverted to the black hole router.

In stark contrast, Talpade explicitly teaches that **all traffic** is redirected to the router filter. Talpade teaches "[t]he new routing information instructs the border and edge routers to reroute all DDoS and non-DDoS traffic directed at the customer network under attack to the filter router using the IP-in-IP tunnels. (See Talpade, para. [0009], emphasis added). As noted above, the Applicants' disclosure teaches that the injected routing instruction contains a second IP address that is the same as the first IP address, but having a higher preference value and a community value. In other words, all traffic is still forwarded to the system under attack. However, once it reaches the system under attack, only some of the traffic is diverted to the black hole router, while the remaining traffic is forwarded to the VPN application. In other words, unlike Talpade, the Applicants' disclosure only diverts a portion of the VPN traffic destined for the system under attack to the black hole router.

The Examiner is reminded that the MPEP § 2141.02(VI) requires the Examiner to consider the prior art in its entirety. "A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention". MPEP § 2141.02(VI), W.L. Gore & Associates, Inc., v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed Cir. 1983), cert. denied, 469 U.S. 851 (1984). Thus, using Talpade with any combination of other references would still teach away from the Applicants' disclosure. The Examiner is expressly prohibited from ignoring those portions of Talpade that explicitly teach away from the Applicants' disclosure.

Moreover, the Examiner concedes that Talpade fails to teach or suggest the above limitation in the Office Action. (See Office Action, p. 3, §4). However, the Examiner asserts that Munger and Official Notice bridge the substantial gap left by Talpade. The Applicants respectfully disagree.

Munger fails to bridge the substantial gap left by Talpade because Munger also fails to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such

that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. The Examiner asserts that the TARP routers taught by Munger are equivalent to a black hole router taught by the Applicants' disclosure. Notably, a black hole router is adapted to black hole traffic (i.e. the traffic is trapped and not forwarded at the black hole router). In stark contrast, the TARP routers by Munger are designed to forward packets randomly to make communication private. (See Munger, col. 7, l. 40 – col. 9, l. 19). That is, the TARP routers taught by Munger do not address "black hole" traffic. Thus, the TARP routers are not equivalent to a black hole router.

In addition, the TARP routers taught by Munger do not inject a second IP address into said ISP VPN network. Rather, Munger teaches that the TARP routers interleave data packets and create new packets that have headers identical to the original data packets. (See Munger, col. 9, ll. 36-50). Notably, the Applicants' claims do not recite creating new packets having a second IP address.

Furthermore, the method taught by Munger would not be practical for the black hole router of the Applicants' disclosure. For example, the Applicants' disclosure is designed to stop attack traffic. Thus, using the method taught by Munger would further slow down the computer network because the router would be required to interleave each one of the thousands of incoming packets during an attack and create new packets for each of the original packets. In stark contrast, the Applicants' disclosure teaches that the black hole router simply injects the second IP address into the ISP VPN network. For example, when routers are identified as potentially being the source of the attack traffic, the second IP address may be injected into the network by updating the routing tables of the routers in question. As a result, the packets do not need to be manipulated, but simply routed based upon the routing protocols of the suspected router or routers.

In addition, the Examiner concedes that Talpade and Munger fail to teach or suggest a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. However, the Examiner asserts Official Notice in asserting that the above limitations are well known in the art as part of BGP protocol.

The Applicants specifically challenge the Examiner's assertion of Official Notice. The Applicants submit that using a higher preference value and a community value for the purpose of selectively black holing data traffic in network is not well known to those skilled in the art. Notably, all of the prior art cited by the Examiner thus far has clearly shown that those skilled in the art at the time of the invention attempted to divert all traffic to the black hole traffic. In stark contrast, the Applicants' disclosure applies the higher preference value and community values in a novel way to selectively divert traffic to black hole routers.

The Examiner is reminded that "Official notice unsupported by documentary evidence should only be taken by the examiner where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known." (See MPEP §21144,03(A), emphasis added). The Applicants request that the Examiner provide a reference that supports the Examiner's use of Official Notice. Thus, the combination of Talpade, Munger and Official Notice fails to render obvious Applicants' independent claims 1, 8 and 15.

In addition, dependent claims 2-7, 10-14 and 16-19 depend from independent claims 1, 8 and 15, respectively, and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 2-7, 10-14 and 16-19 are also patentable over Talpade, Munger and Official Notice and respectfully request the rejection be withdrawn.

CONCLUSION

Thus, the Applicants submit that all of these claims now fully satisfy the requirements of non-statutory obviousness type double patenting and 35 U.S.C. §§ 101 and 103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 842-8110 x130 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully Submitted,

April 5, 2010

Wall & Tong, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 842-8110 x130